HEALTH AFFAIRS

TRICARE Management Activity

DoD Physical Security Requirements

April 2003

HEALTH AFFAIRS

TRRx Physical Security Requirements

TRICARE Management Activity

Statement of Work, Section C:

"**C.14.7**. Information Systems (IS)/Networks Physical Security. The contractor shall employ physical security safeguards for IS/Networks involved in the operation of TRRx program systems of records to prevent the unauthorized access, disclosure, modification, destruction, use, etc., of sensitive information (SI) and to otherwise protect the confidentiality and ensure the authorized use of sensitive information (SI). In addition, the contractor shall support a Physical Security Audit performed by the Government of the contractor's internal information management infrastructure using the criteria from the Physical Security Audit Matrix (Attachment 10, Section J). The contractor shall correct any deficiencies identified by the Government of the contractor's physical security posture."

HEALTH AFFAIRS

Physical Security Requirements

TRICARE Management Activity

1.0 Documentation

– Describes the hardware and software, policies, standards, procedures, and approvals related to physical security.

2.0 Safety

– Evaluates the current state of emergency exits, lights, and insures safety inspections are conducted

HEALTH AFFAIRS

Physical Security Requirements

TRICARE Management Activity

3.0 Physical Access

– Implements access controls that restrict the entry and exit of personnel, equipment and media from the controlled area (e.g., office building, suite, data center, or room).

4.0 Facilities

– Provide protection of the office building, suite, data center, or room where application processing takes place (e.g., doors, locks, windows, etc.)

HEALTH AFFAIRS

Physical Security Requirements

TRICARE Management Activity

5.0 Environmental

– Ensures protection against the loss of electrical power, temperature and humidity control, and fire hazards

6.0 Human Threat

– Ensures protection against internal and external threats by limiting or controlling physical access to the environment

HEALTH AFFAIRS

Physical Security Requirements

TRICARE Management Activity

7.0 Mobile Computing Devices

– Implements protection against unauthorized access to wireless devices, removable media, and sensitive data

8.0 Sensitive Data

– Provides physical protection against unauthorized access to sensitive data

9.0 Hardcopy Output

– Ensures physical protection against unauthorized access to printed products

HEALTH AFFAIRS

Physical Security Requirements

TRICARE Management Activity

10.0 Marking

– Requires appropriate labeling of sensitive data

11.0 Incident Response

– Implements a vulnerability management process for recognizing, responding to, reporting, and mitigating vulnerabilities

Backup Slides

HEALTH AFFAIRS

Physical Security Requirements

TRICARE Management Activity

1.0 Documentation

- **Security Policy (1.1)**
- **Incidence Response Plan (1.2)**
- **Disaster Recovery Plan (1.3)**
- **Access Control (1.4)**
- **Backup Plan (1.5)**
- **Key Control log is maintained (1.6)**

2.0 Safety

- **Emergency Exits (2.1)**
- **Emergency lights with backup power (2.2)**
- **Safety inspection sticker current (2.3)**

HEALTH AFFAIRS

Physical Security Requirements

TRICARE Management Activity

3.0 Physical Access

- Picture Identification Present and Visible (3.1)
- Badge Present and Visible (3.2)
- Visitors Sign In/Out Log (3.3)
- Badge Control Policies In Place (3.4)
- Smart Card/Badge Logs Maintained/Audited (3.5)
- Access Card or Token Swiped for Entry (3.6)
- Key Control Logged/Maintained/Reviewed (3.7)
- Authorized Access List Posted (3.8)
- Data Backup Tapes Securely Stored On-Site (3.9)
- Data Backup Tapes Securely Stored Off-Site (3.10)
- Usage of Storage Media Authorized and Logged (3.11)
- Unattended Terminals Password Protected (3.12)
- Password Protection Automatic w/15 Mins. Inactivity (3.13)

HEALTH AFFAIRS

Physical Security Requirements

TRICARE Management Activity

4.0 Facilities

- **Windows Protected by IDS (< 18' from ground or roof) (4.1)**
- **Openings Covered By Wall, Bars, or 18 Gauge Mesh (> 96 sq in) (4.2)**
- **Individual Personnel Access Enforced (no piggy-backing) (4.3)**
- **Entrance Doors Constructed of Solid Wood, Metal, or Metal Clad (4.4)**
- **Emergency Doors Will Not Allow Entrance (4.5)**
- **Emergency Doors Equipped w/Emergency Bar Openers and Deadbolt Throw (4.6)**
- **Doors Hinged On Inside (4.7)**
- **Magnetic Alarm Switches (Motion Detectors) Installed on Moveable Openings (> 96 sq in) (4.8)**
- **Walls Must Be Solid and True Floor to Ceiling (4.9)**
- **Walls Constructed of Material That Would Provide Detection of Surreptitious Entry (4.10)**
- **Building/Secure Areas Protected w/True Ceilings and Floors (4.11)**
- **Roving Guard (4.12)**
- **Security Lighting for All Exterior Doors (4.13)**

HEALTH AFFAIRS

Physical Security Requirements

TRICARE Management Activity

5.0 Environmental

- **Appropriate Fire Extinguishers Present w/Current Inspections (5.1)**
- **Heat Ventilation Air Conditioning (HVAC) Present and Working (5.2)**
- **Water Sprinklers Present and Working (5.3)**
- **Heat and Smoke Sensors Present and Working (5.4)**
- **Uninterrupted Power Supply (UPS) Present and Working (5.5)**
- **24-Hour Temperature Monitor/Alarm Present and Working (5.6)**

6.0 Human Threat

- **Internal Threat Policies/Procedures in Place (6.1)**
- **External Threat Policies/Procedures in Place (6.2)**
- **Sabotage Policies/Procedures in Place (6.3)**
- **Power Outage Policies/Procedures in Place (6.4)**

HEALTH AFFAIRS

Physical Security Requirements

TRICARE Management Activity

7.0 Mobile Computing Devices

- **Unattended Portable/Wireless Devices Secured and Locked (7.1)**
- **Unattended Removable Media Secured and Locked (7.2)**

8.0 Sensitive Data

- **Sensitive Data Erased From Whiteboards, Removed From Unsecured Areas, and Properly Disposed Of (8.1)**

9.0 Hard Copy Output Access

- **Hard Copy Sensitive Information Shredded or Destroyed (9.1)**
- **Sensitive Hard Copy Output Immediately Retrieved From Output Devices (9.2)**
- **Sensitive Hard Copy Output Secured and Locked (9.3)**

Physical Security Requirements

10.0 Marking

- **Sensitive Data Marked with Security Label (10.1)**

11.0 Incident Response

- **Incident Response Plan/Procedure (11.1)**
- **Computer Emergency Response Team (CERT) (11.2)**

HEALTH AFFAIRS

DITSCAP/Requirements

TRICARE Management Activity

3. Enclave and Computing Environment

- Audit Trail, Monitoring, Analysis and Reporting (3.1)
- Changes to Data (3.2)
- Instant Messaging (3.3)
- Network Device Controls (3.4)
- Privileged Account Control (3.5)
- Production Code Change Controls (3.6)
- Audit Reduction and Report Generation (3.7)
- Security Configuration Compliance (3.8)
- Software Development Change Controls (3.9)
- Transmission Integrity Controls (3.10)
- Audit Trail Protection (3.11)
- Voice over Internet Protocol (3.12)
- Virus Protection (3.13)
- Wireless Computing and Networking (3.14)
- Affiliation Display (3.15)
- Access for Need-to-Know (3.16)
- Audit Record Content (3.17)
- Encryption for Confidentiality (Data at Rest) (3.18)

HEALTH AFFAIRS

DITSCAP/Requirements

TRICARE Management Activity

3. Enclave and Computing Environment (Cont.)

- **Encryption for Confidentiality (Data in Transit), (3.19)**
- **Interconnections among DoD Systems and Enclaves (3.20)**
- **Logon (3.21)**
- **Least Privilege (3.22)**
- **Marking and Labeling (3.23)**
- **Conformance Monitoring and Testing (3.24)**
- **Encryption for Need-To-Know (3.25)**
- **Resource Control (3.26)**
- **Audit Record Retention (3.27)**
- **Tempest Control (3.28)**
- **Warning Message (3.29)**
- **Account Control (3.30)**

HEALTH AFFAIRS

DITSCAP/Requirements

TRICARE Management Activity

4. Enclave Boundary Defense

- **Boundary Defense (4.1)**
- **Connection Rules (4.2)**
- **Virtual Private Network Controls (4.3)**
- **Intrusion Detection (4.4)**
- **Public WAN Connection (4.5)**
- **Remote Access for Privileged Functions (4.6)**
- **Remote Access for User Functions (4.7)**